



Department of Homeland Security National Infrastructure Protection Center

Daily Open Source Infrastructure Report for 20 March 2003

Current Nationwide
Threat Level is



[For info click here](#)

www.whitehouse.gov/homeland

Daily Overview

- The Miami Herald reports that authorities in Key West arrested six Cuban men Wednesday night after they allegedly hijacked a Cuban domestic flight at knife point; the plane and landed safely in Key West under the escort of U.S. fighter jets. (See item [8](#))
- CNN reports the Federal Aviation Administration, in conjunction with the government raising the terrorism threat level in the U.S. to orange, has announced new flight restrictions for both commercial and private aircraft flying in the New York City and Washington, D.C. areas, and near Disney World and Disneyland. (See item [11](#))
- The General Accounting Office has released its report GAO-03-342, entitled "Food-Processing Security: Voluntary Efforts Are Underway, but Federal Agencies Cannot Fully Assess Their Implementation." (See item [22](#))
- Microsoft has released "Security Bulletin MS03-008: Flaw in Windows Script Engine Could Allow Code Execution (Critical)," and a patch is available at the Microsoft website. (See item [32](#))
- CERT has released "Advisory CA-2003-10: Integer overflow in Sun RPC XDR library routines," which will lead to denial of service, execution of arbitrary code, or the disclosure of sensitive information. (See item [34](#))
- eWEEK reports the MIT Kerberos development team says the contents of an unpublished paper with details about a serious weakness in MIT's Kerberos v4 authentication protocol has been leaked on the Internet. (See item [35](#))

DHS/NIPC Update *Fast Jump*

Production Industries: [Energy](#); [Chemical](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [General](#); [DHS/NIPC Web Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: High, Cyber: High

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://esisac.com>]

1. *March 19, Reuters* — **U.S. Senate rejects oil drilling in Alaskan refuge. The U.S. Senate narrowly voted Wednesday to maintain a ban on oil drilling in the Arctic National Wildlife Refuge.** The Senate vote struck language attached to the 2004 budget resolution that would have opened the Alaska refuge to drilling and collected more than \$2 billion in leasing fees from oil companies. Republicans added the provision to the budget resolution because it needs only 50 votes to pass, unlike most controversial bills which require 60 votes to end debate before a floor vote. **The White House wants to tap the refuge's potential 16 billion barrels of crude to help reduce U.S. dependence on foreign oil imports.**
Source: <http://www.forbes.com/personalfinance/retirement/newswire/2003/03/19/rtr912120.html>
2. *March 18, Lexington Herald-Leader* — **Three Kentucky electricity plants to burn landfill gas, not coal.** Construction will begin soon on three plants that will convert landfill gas into electricity. **The plants will be the first of their kind in Kentucky. Instead of coal, they will burn methane and other landfill gases to generate electricity.** East Kentucky Power Cooperative will build the plants at the Bavarian Landfill in Boone County, the Laurel Ridge Landfill in Laurel County and the Green Valley Landfill in Greenup County. **Each of the 5,000-square-foot plants will cost \$4 million and generate a combined 10 megawatts of power. That's enough, East Kentucky Power says, to supply power to all the homes in two cities the size of Shelbyville. The gas is produced by decaying trash. It now escapes into the the atmosphere, where it becomes a greenhouse gas and possibly contributes to global warming.** Converting landfill gas into electricity costs more than converting coal, however, and that cost is passed on to customers through the co-op's EnviroWatts program. Some customers already are enrolled in the program, using "green" power generated at landfills in Indiana. Customers pay an extra \$2.75 a month for each block of 100 kilowatt hours of green energy they choose to buy. An average customer uses about 1,000 kilowatt hours a month, and has a bill of about \$60. If that customer decided to buy one 100 kilowatt-hour block of green power, the bill would be \$62.75.
Source: http://www.energycentral.com/sections/news/nw_article.cfm?id=3718263
3. *March 18, XINHUA – WorldSources Online* — **Power cut off again in parts of southern Philippines. A massive electric power outage on Tuesday hit a number of cities in Mindanao in the southern Philippines a week after rebels toppled transmission lines, officials said. Several million people were without power, the ABS-CBN news channel quoted officials at the state-run National Power Corp. They were not ruling out sabotage by rebel Moro Islamic Liberation Front (MILF) rebels, who blew up power pylons last week to cut off electricity to 90 percent of the island of 18 million.** "I believe there is a transmission tower toppled down, but we are unsure where the exact location is," said Jojo Palma, a Napocor manager. He said four provinces were without electricity and the power is expected to be fully restored in two to three hours.

[\[Return to top\]](#)

Chemical Sector

4. *March 19, United States Chemical Safety and Hazard Investigation Board* — **Fire forces evacuations, destroys Indiana plant. A Franklin, IN metal plating plant burned to the ground early this morning in a fire that forced the evacuation of a nearby subdivision, delayed the opening of Franklin Community Schools and left a massive cleanup for environmental crews.** Franklin Fire Dept. Capt. Ron Macy said the fire was reported at the Electro-Spec plant on Earlywood Drive, in an industrial area north of the city, about 4 a.m. When firefighters arrived about four minutes later, heavy smoke was pouring from the building, and the seven employees known to be working inside the building were outside and uninjured. **Due to the hazardous chemicals stored in the building's warehouse and plating shop areas, firefighters followed a pre-planned response, allowing the fire to burn but containing it, Macy said.** Assistant Franklin Fire Chief Jim Reese said the 12,500-square-foot building did not have an automatic fire suppression system and was built before code required it. Electro-Spec specializes in the electroplating of electronic parts with metal coatings such as gold, silver and specialized alloys. **It stored at its plant several thousand pounds of caustic chemicals such as sulfuric acid, nitric acid and sodium hydroxide and toxic chemicals such as copper cyanide and sodium cyanide.** Shortly after the fire began, firefighters began knocking on doors in Branigin Creek, a subdivision of several dozen homes across U.S. 31 but downwind of the fire, and advising residents to evacuate. **Macy said firefighters and inspectors with the Johnson County Board of Health were checking the air quality in surrounding neighborhoods.**

Source: http://www.chemsafety.gov/circ/post.cfm?incident_id=6448

[\[Return to top\]](#)

Defense Industrial Base Sector

5. *March 19, Los Angeles Times* — **The delicate choreography of supplying America's troops.** The port of Jacksonville, Florida has become a major transit hub for military equipment bound for the U.S. troops poised to invade Saddam Hussein's country, with hundreds of armored vehicles, trucks, bulldozers, Humvees and other olive-drab and buff combat machines lined up to be loaded into ships. **Logistically, the operation is already a success, according to the U.S. Transportation Command, the military's umbrella agency for shipping people, weapons, ammunition, food and other supplies. The buildup ordered by President Bush has taken a third less time than the six months spent moving forces and gear to prepare for the 1991 Persian Gulf War, said Air Force Gen. John W. Handy, head of the Transportation Command.** The large-scale delivery operation hasn't been without bottlenecks and other problems. But military logisticians say it is functioning faster and more efficiently because of lessons learned in Operation Desert Storm, as well as improved computer and satellite technology and the \$6 billion spent on a new generation of Navy transport ships that can hold 3,200 mid-sized sport utility vehicles each.

Source: <http://www.latimes.com/news/nationworld/iraq/homefront/la-wa-r-logistics19mar19,1,821235.story>

6. *March 16, Farmington Daily Times* — **New command to guard homeland says it faces changing threats.** The head of the new Colorado-based military command that is responsible for protecting the U.S. gave Congress an optimistic assessment of its startup on Thursday March 13th, but acknowledged that the command "will never reach full operational capability" because the threats are constantly changing. **Gen. Ralph E. "Ed" Eberhart sought to assure the House Armed Services Committee his five-month old U.S. Northern Command is "further along than I thought it would be" coordinating the military's response to possible threats. "We have to continue to get better, to stay ahead of the bad guy, if you will," he said.** But while many lawmakers praised the general, they questioned whether the country has done enough to guard against the terrorists threats posed by missiles, chemical-laden drones and container ships. Eberhart replied that the answer is likely to be in better technology that would detect such threats before they reached the U.S. "We think, sadly, we're more likely to face an attack like we did on 9/11 whether it's from the air, land or sea, from a terrorist, or some sort of copy cat," he said. **What's different now, he argued, is his command, which was activated Oct. 1 at Peterson Air Force Base. "Day and day out (it) focuses on nothing but homeland defense and homeland security," he said.**

Source: <http://www.daily-times.com/Stories/0,1413,129%257E6574%257E1248076,00.html?search=filter>

[[Return to top](#)]

Banking and Finance Sector

7. *March 19, Washington Post* — **Terrorism and the markets. Senior Treasury Department officials said today that since the Sept. 11, 2001, terrorist attacks, the federal government has stepped up efforts to protect financial markets and the banking system, but they warned that a major attack could still cause disruptions.** "We know terrorists are trying to strike us as a world financial center, and in order to counter that we need to be able to demonstrate that the U.S. is a reliable place to engage in financial transactions," one Treasury official said, speaking on the condition that he not be named. The officials added that Treasury has developed several alternative lines of communication between the government and bond market participants to ensure that debt sales are not interrupted. After the Sept. 11 attacks, bond trading was halted for two days and the government postponed debt sales. **The bond market had a value of \$20.2 trillion at the end of 2002, with government securities making up \$3.2 trillion of that, according to the Bond Market Association. Federal, state and local governments rely on bond sales to fund operations and provide liquidity to the marketplace. Companies rely on bond sales to raise capital.**

Source: <http://www.washingtonpost.com/wp-dyn/articles/A49423-2003Mar 18.html>

[[Return to top](#)]

Transportation Sector

8. *March 20, Miami Herald* — **Cuban plane flown to U.S.; six arrested in hijacking.** Authorities in Key West arrested six Cuban men Wednesday night after they allegedly hijacked a Cuban domestic flight at knife point. The plane, carrying 37 people including the alleged hijackers, landed safely in Key West under the escort of U.S. fighter jets. The scheduled flight, a normally brief Cuban Aerotaxi route from Cuba's Isle of Youth to Havana, had been diverted north toward Florida when it was spotted at 7:42 p.m. by air-traffic controllers in Miami, according to the Federal Aviation Administration. Six men in their 20s from the Isle of Youth produced four kitchen knives and said they wanted to go to Key West. Fighter jets from Homestead Air Reserve Base escorted the plane to a runway at Key West International Airport at 8:06 p.m. **It was met on the runway by officials from the FBI, the Department of Homeland Security and local law enforcement. The alleged hijackers were not immediately identified, nor was their motive.** Also aboard were a pilot, copilot, four other crew members and 25 other passengers — 12 men, eight women and five children. **None were harmed.**
Source: <http://www.miami.com/mld/miamiherald/5434271.htm>
9. *March 19, Washington Post* — **Airlines cut schedules of overseas flights. Several major international airlines began cutting back flight schedules Tuesday in anticipation of a war in Iraq while other carriers said they were prepared to put contingency plans into action as soon as hostilities begin.** British Airways announced that it would suspend daily service between London and Kuwait beginning Wednesday. It also said it was closing its three offices in Kuwait City and will cut back its twice-daily service between London's Heathrow Airport and Tel Aviv to once a day. Swiss International Air Lines said it would reduce its flights from Zurich to Cairo from six to two a week. Continental Airlines, which had already reduced the frequency of its flights from Newark to Tokyo, also announced plans to cut back flights to London from Newark, Houston and Cleveland, and to Paris from Newark, beginning next month. Continental left its daily nonstop flight to Tel Aviv unchanged. **The moves by the jittery airline industry reflect fears that a war in Iraq could push the struggling industry further into financial turmoil. The U.S. airline industry has lost \$18 billion since Sept. 11, 2001, and is projected to lose \$6.7 billion this year even without a war in Iraq, according to the Air Transport Association (ATA), which represents the industry.** Henry H. Harteveldt, an analyst with Forrester Research Inc., said, "I expect within the next 24 hours we'll see airlines announcing major cutbacks in their transatlantic flying." **He said the cutbacks may reach as high as 20 percent.**
Source: <http://www.washingtonpost.com/wp-dyn/articles/A49886-2003Mar 18.html>
10. *March 19, Reuters* — **British police find bombs in raid near airport. British police said on Wednesday they had arrested three men under anti-terrorism laws after finding two explosive devices at a home near Gatwick airport, south of London.** Police said the men, arrested late on Tuesday, were European citizens and that they had not been linked to any specific group or target. "Two explosive devices have been found at an address in Crawley, Sussex, and three men have been arrested and are being questioned," a Sussex police spokeswoman said.
Source: http://dailynews.att.net/cgi-bin/news?e=pri_wsrrodc
11. *March 19, CNN* — **FAA announces code orange flight restrictions. The Federal Aviation Administration Tuesday announced flight restrictions for aircraft flying in the New York**

City and Washington areas, and near Disney World and Disneyland. The restrictions, which affect both commercial and private aircraft, are in conjunction with the government raising the terrorism threat level in the United States from yellow (elevated) to orange (high) as U.S. forces are poised for war in Iraq. **Airspace restrictions announced Tuesday will remain in effect indefinitely, the FAA said. The new regulations in effect create a no-fly zone around Disney World in Orlando, Florida and Disneyland in Anaheim, California. Unless pilots are granted specific exemptions from air traffic controllers, no flights are allowed within a 3-mile radius around the parks or below 3,000 feet.** Government officials said the Disney restrictions are not based on any specific or new information, but rather stem from a general concern about those two locations as possible terror targets. **Also new is the Air Defense Identification Zone, which extends for a 30-mile radius around the New York City area's three major airports: Kennedy, LaGuardia and Newark, New Jersey.** All aircraft in the zone flying below 18,000 feet must have a flight plan and be in continual contact with air traffic controllers through transponders onboard and verbal contact from pilots. More details are available at <http://www2.faa.gov/SPECIALNOTAMS/specialnotamlisting.htm>
Source: <http://www.cnn.com/2003/TRAVEL/03/18/airspace.restrictions/index.html>

12. *March 19, Washington Post* — **Mall standoff fuels evacuation fears.** Washingtonians already worried about escaping the District in a terrorist attack said **their fears grew Tuesday when they saw how easily one man on a tractor brought rush-hour traffic in and around the city to a standstill.** By early Tuesday evening, a third rush hour had been turned into a maddening mess by the police standoff that closed much of Constitution Avenue, a key downtown artery, and several intersecting streets. **Area emergency planners said the incident underscored their warnings that the region's fragile transportation network, overwhelmed during a normal rush period, would buckle in a crisis. In a terrorist attack, most people would be asked to "shelter in place,"** leaving roads and transit free for emergency workers and those fleeing the immediate area of the attack. Planners said Tuesday's tie-ups also showed that people need quicker, clearer instructions when incidents affect their mobility.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A49354-2003Mar 18.html>

[[Return to top](#)]

Postal and Shipping Sector

13. *March 19, Times Picayune* — **Ports, plants boost security.** With war imminent in Iraq and the United States' terror alert level ratcheted back up to orange, **local and state officials stepped up security measures Tuesday at Louisiana port facilities, water-treatment plants and other buildings that could be enticing targets for mayhem.** Terry Ebbert, New Orleans homeland security director, said **the region could be a tempting target for terrorists because of port facilities and the concentration of petrochemical plants and pipelines along the Mississippi River.** Local maritime officials responded quickly to the raised security alert. **The Port of New Orleans began stationing a Harbor Police officer at each of the four entry gates to the port's Uptown cargo terminals,** said Cynthia Swain, the port's director of safety and security. The officers joined private security guards who will continue operating the gates for the port. **Guards also began stopping every vehicle entering the terminals and checking the identification of each driver,** Swain said. Previously, guards allowed vehicles with port

identification decals to pass without stopping. Swain said she couldn't estimate how long the security changes at the port would be in place, except to say they likely would remain until hostilities wane. **The Coast Guard, meanwhile, increased patrols by cutters and helicopters along the lower Mississippi,** Coast Guard Petty Officer Jonathan F. McCool said. He said security concerns prevented him from discussing specifics. **He repeated previous requests for people working along the river to report any unusual or suspicious activity by calling the Coast Guard's local 24-hour command center at (504) 589-6225.**

Source: http://www.nola.com/news/t-p/index.ssf?/base/news-0/10480587_32320860.xml

14. *March 19, New York Times* — **Cargo insurance would end 48 hours into an Iraqi war. International insurance companies notified the world's airlines and the operators of oil tankers and cargo ships Tuesday that their coverage for wartime cargo losses in the Middle East would be canceled within 48 hours of the start of any hostilities in Iraq.** The coverage can be renegotiated, insurance brokers said, but at much higher prices. Some brokers said they regarded the decision on cargo as a precursor to a broader cancellation notice for coverage on the airliners and ships themselves. The brokers said that the new prices could be as much as 50 times the prewar prices for cargo coverage and that costs of war coverage for aircraft and ships could easily increase tenfold for a single voyage or flight. **As a result, they said, most commercial air and sea traffic to the Persian Gulf region would probably be halted.**

Source: <http://www.nytimes.com/2003/03/19/business/worldbusiness/19INSU.html>

15. *March 19, Department of Homeland Security* — **U.S. Coast Guard announces temporary final rule establishing security zones in San Francisco Bay. The U.S. Coast Guard is establishing fixed security zones extending 25 yards in the U.S. navigable waters around all piers, abutments, fenders and pilings of the Golden Gate Bridge and the San Francisco–Oakland Bay Bridge, San Francisco Bay, California.** These security zones are needed for national security reasons to protect the public and ports from potential subversive acts. **Entry into these security zones is prohibited, unless doing so is necessary for safe navigation, to conduct official business such as scheduled maintenance or retrofit operations, or unless specifically authorized by the Captain of the Port San Francisco Bay, or his designated representative.** This regulation is effective from 11 a.m. PST on February 13, 2003 to 11:59 p.m. PDT on September 30, 2003.

Source: <http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2003/03-6630.htm>

16. *March 19, Department of Homeland Security* — **U.S. Coast Guard announces final rule establishing security zone for liquefied hazardous gas tank vessels in San Pedro Bay, CA. The U.S. Coast Guard is revising current safety zone regulations by establishing security zones around and under all liquefied hazardous gas (LHG) tank vessels located on San Pedro Bay, California, in and near the ports of Los Angeles and Long Beach.** These security zones are needed for national security reasons to protect the public and ports from potential subversive acts. **Entry into these zones will be prohibited unless specifically authorized by the Captain of the Port Los Angeles–Long Beach. This rule is effective March 21, 2003.**

Source: <http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2003/03-6632.htm>

17. *March 18, Government Executive* — **Customs officials intensify efforts against illicit tech exports.** Customs officials have intensified efforts to block shipments of controlled military technologies to Iraq and other nations deemed as threats, according to David Conboy, assistant director of strategic investigations at the Bureau of Immigration and Customs Enforcement. **He said that to bring a criminal case against an illicit exporter, officials have to show there was intent to break the law. They must show the exporter knew the law and did something to circumvent it.** Conboy described an undercover sting operation that netted an Iraqi selling military equipment from the United States to Iraq. Fadi Boutros had immigrated from Iraq and established a front company in San Diego. It acted as a procurement agent, reaching out to U.S. companies seeking various technologies, some controlled by the government. **In its years-long undercover operation in the late 1990s, Customs discovered the front company had a "shopping list" of goods being sought by Iraq, including software for a ballistic missile guidance system and other military items. For instance, the company also sought 20 pairs of the most advanced night vision goggles in the world, made only in the United States at that time.** Customs tapped the company saying it knew it could not get a license to ship the items and that it would get around it. In its order, the company paid \$30,000 up front and gave specific instructions on how it would avoid detection. This included requesting labeling the shipment as an "ophthalmoscope," and valuing it at \$100, instead of the tens of thousands it was worth. When the exporter showed up to FedEx to make the shipment, he was arrested. Source: <http://www.govexec.com/dailyfed/0303/031803td1.htm>

[[Return to top](#)]

Agriculture Sector

18. *March 19, Associated Press* — **New disease threatens Brazil's oranges. A new citrus disease called Sudden Death could destroy almost all of Brazil's orange groves if left unchecked, officials and agricultural experts said. The warning was issued Tuesday at the start of a campaign aimed at combating a disease that has killed about 3 million trees since it was first detected three years ago in the southern state of Minas Gerais. The disease since has spread into the state of Sao Paulo, which has 85 percent of Brazil's 280 million orange trees. Brazil is the world's largest orange producer and exporter of frozen concentrate orange juice. ``We have to act fast," said Ademerval Garcia, president of the Brazilian Citrus Exporters Association. ``If we don't we could see most of our oranges wiped out." No cure has been found for the disease, which can kill a tree one or two weeks after the first symptoms appear. While the cause has not been established, private citrus research foundation Fundecitrus believes it is a mutation of the Tristeza citrus virus that wiped out 9 million of Brazil's 11 million orange trees in 1940.** Source: http://www.news-journal.com/news/content/news/ap_story.html/Intl/AP.V5537.AP-Brazil-Oranges.html

19. *March 19, Daily Pennsylvanian* — **Vets map farms to track possible bioterrorism.** Pennsylvania farms, with the help of the University of Pennsylvania's School of Veterinary Medicine, have become tools in the tracking of potential bioterrorism. A group of faculty members from the School's New Bolton Center is conducting a program for the mapping of animal farms in Pennsylvania. "The goal is to map every kind of farming

enterprise in the Commonwealth of Pennsylvania," said Population Biology and Epidemiology Professor Gary Smith. "Knowing where the animals are is key," Pennsylvania State Veterinarian John Enck said. The group running the project is called the Epidemic Disease Geographical Information System Unit, which is funded by the Pennsylvania Department of Agriculture and composed of a dozen faculty members of the Vet School. The mapping will cover only those industries that deal with animals. **Once the researchers collect all the data, they will use them to run computer simulations of the spread of diseases and infections in animals. The methodology used for this project can also be employed to monitor possible instances of bioterrorism. As with natural diseases, researchers can devise possible scenarios in different kinds of situations.**

Source: <http://www.dailypennsylvanian.com/vnews/display.v/ART/2003/03/19/3e783c1513755>

[[Return to top](#)]

Food Sector

20. *March 19, Food Production Daily* — **Bacteria may protect cheese from listeria. German researchers have found that the addition of a bacterium during cheese production may be a simple answer to preventing listeria in unpasteurised produce.** In the study, cheese was ripened with or without the bacterium *Lactobacillus plantarum*. The results showed complete inhibition to listeria bacteria in the cheese produced with *L. plantarum*. The reason for the inhibition appears to be a compound produced by *L. plantarum* called pediocin. **The authors did express a mild concern over an observation that in some cases listeria may become resistant.**

Source: <http://www.foodproductiondaily.com/news/news.asp?id=2481>

21. *March 19, Reuters* — **U.S. food plants, stockyards step up security. Food processors, grain elevators, and stockyards are tightening security to protect the U.S. food supply from possible sabotage as Washington prepares to take military action against Iraq, the Bush administration said on Tuesday.** The U.S. Agriculture Department (USDA) separately urged food plants, farms, grain elevators and other agribusinesses to inspect all trucks and cars entering their property and to escort visitors. **The USDA said it has hired 20 new food security inspectors based at "strategic points of entry" into the United States. The department also placed on stand-by several special teams of experts who can immediately travel to an emergency site to help manage any food or livestock contamination.** The USDA security directive can be found at

<http://www.fsis.usda.gov/OPPDE/rdad/FSISDirectives/5420.1.pdf>.

Source: <http://asia.reuters.com/newsArticle.jhtml?type=politicsNews&storyID=2400815>

22. *March 18, General Accounting Office* — **Food-Processing Security: Voluntary Efforts Are Underway, but Federal Agencies Cannot Fully Assess Their Implementation.** The General Accounting Office (GAO) has released report GAO-03-342, entitled "Food-Processing Security: Voluntary Efforts Are Underway, but Federal Agencies Cannot Fully Assess Their Implementation." **GAO found that federal food safety statutes give the Food and Drug Administration (FDA) and the U.S. Department of Agriculture (USDA) broad authority to regulate the safety of the U.S. food supply but do not specifically authorize them to**

impose security requirements at food-processing facilities. FDA believes that its statutes authorize it to regulate food security to the extent that food security and safety overlap but observes that there is little overlap between security and safety. USDA believes that it could require food processors to adopt certain security measures that are closely related to sanitary conditions inside the facility. **USDA also believes that the statutes cannot be interpreted to authorize the regulation of security measures that are not associated with the immediate food-processing environment, such as requiring fences, alarms, and outside lighting.** Neither agency believes that it has the authority to regulate all aspects of security at food-processing facilities. **Both FDA and USDA issued voluntary security guidelines to help food processors identify measures to prevent or mitigate the risk of deliberate contamination.** Since FDA and USDA do not monitor and document food processors' implementation of security guidelines, the extent of the industry's adoption of security measures is unknown. According to officials of trade associations and the five facilities that the GAO visited, food processors are implementing a range of security measures. **In addition, the FDA and USDA field inspectors that the GAO surveyed indicated that most facilities have implemented some security measures, such as installing fences. However, the inspectors were less able to comment on security measures that were not as obvious, such as accounting for missing stock and implementing proper mail-handling practices.** Highlights are available at <http://www.gao.gov/highlights/d03342high.pdf>
Source: <http://www.gao.gov/new.items/d03342.pdf>

[[Return to top](#)]

Water Sector

23. *March 19, Bangkok Post* — **MILF rebels bomb main water pipeline. Muslim separatist rebels Wednesday bombed a main water pipeline in a southern Philippine city in the latest in a series of attacks by the guerrillas, a military official said.** Major Julieto Ando, a regional army spokesman, said no one was hurt when Moro Islamic Liberation Front (MILF) rebels exploded before dawn two bombs at the main water pipeline in Kidapawan City, North Cotabato province, 930km south of Manila. **"There were no reports of civilian casualties, but the blasts cut off the water supply in Kidapawan and five outlying villages," he said.** Source: http://www.bangkokpost.com/News/20Mar2003_news32.html

[[Return to top](#)]

Public Health Sector

24. *March 19, Washington Post* — **Tests suggest virus link. Scientists have found evidence of a virus in at least two patients stricken by the mysterious respiratory infection that has triggered a global health alert, officials said Tuesday. Laboratories in Germany and Hong Kong testing samples from victims found signs of a microbe known as a paramyxovirus, a family of viruses that can cause a spectrum of diseases in animals and humans, officials said.** Some paramyxoviruses can cause relatively mild respiratory illness. Others cause well-known ailments such as mumps and measles, and still others are responsible for exotic, deadly respiratory infections that emerged in Asia and Australia in the 1990s, officials said.

Although the discovery could be a major break in the hunt for the cause of the global outbreak, officials cautioned that the findings were preliminary and that the virus could have nothing to do with the disease, which is dubbed severe acute respiratory syndrome (SARS).

Source: http://www.washingtonpost.com/wp-dyn/articles/A49172-2003Mar_18.html

25. *March 19, Associated Press* — **Thompson says officials checking out reports of mystery illness in U.S. Health and Human Services Secretary Tommy Thompson says authorities are checking to see if that fast-moving mystery illness has hit the U.S. He told senators the government is investigating 40 reports in the U.S. of the virus, and is looking carefully at eleven of those.** Thompson says there's still no confirmation that the mystery illness is a virus. U.S. scientists, he adds, are now studying specimens they've just received from overseas.

Source: <http://www.wpmi.com/Global/story.asp?S=1186657>

[[Return to top](#)]

Government Sector

26. *March 19, New York Times* — **Higher alert and tighter budgets.** As the nation returned to a high level of alert, state, local and federal officials stepped up security Tuesday at sensitive sites. But many states stopped short of activating the National Guard, despite the Bush administration's call for governors to deploy such troops or state police. Even as Tom Ridge, the secretary of homeland security, announced plans to safeguard everything from ports to air travelers to food supplies, **many state domestic security chiefs and local emergency managers were still trying to find the right balance for a time of war and tight budgets.** "If we know of a threat we will meet it and deal with the checkbook later," said Clifford Ong, director of Indiana's Counter-Terrorism and Security Council, "but absent a threat, we have to make real decisions on what we can do with National Guard and state police overtime. **Of 31 states surveyed by reporters on Tuesday, six had deployed the National Guard. Officials in Indianapolis and New Orleans began planning for tightened security at this weekend's N.C.A.A. basketball tournaments – Louisiana officials said the state would use its National Guard troops, as it did for the Super Bowl and Mardi Gras.** Amid the worst fiscal crises since World War II, most states held off activating their emergency operations centers, an expensive proposition, at least until the shooting starts.

Source: <http://www.nytimes.com/2003/03/19/national/19SECU.html>

27. *March 19, CNN* — **Official warns of 'multiple' al Qaeda attacks.** Cofer Black, the State Department coordinator for counterterrorism, told the Senate Foreign Relations committee that **al Qaeda is "still dangerous, still vicious, but I would say things are not going well for the terrorists."** He said leaders from Osama bin Laden down currently **"spend more time trying to figure out how to keep from getting caught than they do trying to launch operations."** Black said that in addition to the recent capture of al Qaeda operations chief Khalid Shaikh Mohammed, the seizure of another, lower level al Qaeda figure is also likely to reap intelligence benefits. Yassir al-Jaziri was captured Saturday in Pakistan. Black told CNN he is "a second-tier guy but one who knows things."

Source: <http://www.cnn.com/2003/US/03/18/sprj.iqr.terror.alert/index.html>

28. *March 19, Washington Post* — **Security tightens across nation; asylum seekers to be detained.** The Homeland Security Department announced Monday a temporary policy under which **newly arriving applicants for asylum from 33 nations where terrorists or their sympathizers have operated will be jailed until their cases are adjudicated. The policy also includes newly arriving asylum seekers from the West Bank and Gaza.** U.S. officials said that about 600 people seek asylum from the 33 nations in question each year, and about 60 percent of them are from Iraq. Homeland Security officials said they want to ensure that Iraq does not dispatch secret agents posing as asylum seekers to conduct terror strikes.

Source: http://www.washingtonpost.com/wp-dyn/articles/A49400-2003Mar_18.html

29. *March 19, Honolulu Advertiser* — **Hawaii terror-alert level remains at lower status.** While the state's terror-alert level stayed blue yesterday, Gov. Linda Lingle said it might go to yellow, and airport and harbor officials already were acting like it's orange. **The state will stay, for now, at the second-lowest blue alert level, even though President Bush has warned that the United States should expect a terrorist response in the event of military action in Iraq. The state's terror-alert level could rise to yellow if the nation goes to war, Lingle said on Tuesday.** At state airports, harbors and military bases, however, officials put extra security measures into practice in line with the increased federal alert level. **"At the airports and harbors, we follow the federal mandate, which is orange right now,"** said Rod Haraga, state transportation director.

Source: http://the.honoluluadvertiser.com/article/2003/Mar/19/lh/ln0_4a.html

[[Return to top](#)]

Emergency Services Sector

30. *March 19, New York Times* — **Air patrols and officers at TV stations as New York goes on alert.** As the nation inched closer to war, Mayor Michael R. Bloomberg said on Tuesday that **federal authorities had agreed to secure New York City's airspace and provide military air patrols as part of a broad Police Department plan to safeguard against attacks.** Bloomberg described the department's war contingency plan, Operation Atlas, as the most comprehensive terrorism prevention effort the city has ever conducted. The plan, first disclosed over the weekend and expected to cost at least \$5 million a week in police overtime, **includes expanded patrols on the streets, focusing on government buildings, tourist attractions, financial institutions, hotels and houses of worship, and in the subways, on the waterways and in the harbor. It will also strengthen checkpoints at bridges and tunnels and on the streets, including southbound avenues in Manhattan at 96th Street.** Officials said that among other measures, there would be extra patrols in Jewish neighborhoods deemed to be terrorist targets, 24-hour police coverage of Wall Street, harbor patrols to protect commuter ferries and bomb-sniffing dogs on the Staten Island Ferry. Officers will also be posted outside television news outlets to prevent possible takeovers by terrorists who may want to broadcast anti-American messages.

Source: <http://www.nytimes.com/2003/03/19/nyregion/19KELL.html>

31. *March 19, Washington Times* — **District steps up measures over terror alert.** The U.S. Secret Service widened perimeters around the White House, the U.S. Coast Guard stepped up patrols on the Potomac River and the Metropolitan Police Department

activated its Joint Operations Command Center yesterday in response to a heightened terrorism alert. Other measures included putting U.S. Park Police officers on duty around national monuments, having more officers carry machine guns, increasing visibility of SWAT teams, searching vehicles at area airports and calling on residents to be extra vigilant. **"We have to be vigilant, but we can't panic," said D.C. Mayor Anthony A. Williams. "We have to have an open city, but we have to have a safe city. We can do both."** D.C. Police Chief Charles H. Ramsey mobilized the Joint Operations Command Center and said the center's 14 security cameras would be activated "as long as it is Code Orange."

Source: <http://www.washingtontimes.com/metro/20030319-90176914.htm>

[\[Return to top\]](#)

Information and Telecommunications Sector

32. *March 19, Microsoft* — **Microsoft Security Bulletin MS03-008: Flaw in Windows Script Engine Could Allow Code Execution.** The Windows Script Engine provides Windows operating systems with the ability to execute script code. **A flaw exists in the way by which the Windows Script Engine for JScript processes information. An attacker could exploit the vulnerability by constructing a web page that, when visited by the user, would execute code of the attacker's choice with the user's privileges.** The web page could be hosted on a web site, or sent directly to the user in email. Exploiting the vulnerability would allow the attacker only the same privileges as the user. **Computers configured to disable active scripting in Internet Explorer are not susceptible to this issue.** Users whose accounts are configured to have few privileges on the system would be at less risk than ones who operate with administrative privileges. Automatic exploitation of the vulnerability by an HTML email would be blocked by Outlook Express 6.0 and Outlook 2002 in their default configurations, and by Outlook 98 and 2000 if used in conjunction with the Outlook Email Security Update. **Microsoft has assigned a risk rating of "Critical" to this vulnerability. A patch is available at the Microsoft Website. Microsoft has also provided information about preventive measures customers can use to help block the exploitation of this vulnerability while they are assessing the impact and compatibility of the patch.**

Source: <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-008.asp>

33. *March 19, Microsoft* — **Microsoft Security Bulletin MS03-009: Flaw In ISA Server DNS Intrusion Detection Filter Can Cause Denial Of Service.** Microsoft Internet Security and Acceleration (ISA) Server 2000 contains the ability to apply application filters to incoming traffic. **A flaw exists in the ISA Server DNS intrusion detection application filter, and results because the filter does not properly handle a specific type of request when scanning incoming DNS requests. An attacker could exploit the vulnerability by sending a specially formed request to an ISA Server computer that is publishing a DNS server, which could then result in a denial of service to the published DNS server.** DNS requests arriving at the ISA Server would be stopped at the firewall, and not passed through to the internal DNS server. All other ISA Server functionality would be unaffected. By default, no DNS servers are published. DNS server publishing must be manually enabled. The vulnerability would not enable an attacker to gain any privileges on an affected ISA Server or the published DNS server or to compromise any cached content on the server. It is strictly a

denial of service vulnerability. **Microsoft has assigned a risk rating of "Moderate" to this vulnerability. A patch is available at the Microsoft website.**

Source: <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-009.asp>

- 34. *March 19, CERT/CC* — CERT Advisory CA-2003-10: Integer overflow in Sun RPC XDR library routines.** XDR (external data representation) libraries are used to provide platform-independent methods for sending data from one system process to another, typically over a network connection. **The `xdrmem_getbytes()` function in the XDR library provided by Sun Microsystems contains an integer overflow that can lead to improperly sized dynamic memory allocation.** Depending on how and where the vulnerable `xdrmem_getbytes()` function is used, **subsequent problems like buffer overflows may result. Exploiting this vulnerability will lead to denial of service, execution of arbitrary code, or the disclosure of sensitive information.** Specific impacts reported include the ability to crash the `rpcbind` service and possibly execute arbitrary code with root privileges. In addition, intruders may be able to crash the MIT KRB5 `kadmind` or cause it to leak sensitive information, such as secret keys. **CERT recommends the application of a vendor specified patch or upgrade as specified by vendor.**



Source: <http://www.cert.org/advisories/CA-2003-10.html>

- 35. *March 17, eWEEK* — Details of Kerberos vulnerability leaked.** There is a serious weakness in MIT's Kerberos v4 authentication protocol that allows an attacker to impersonate any principal in a given realm. The Kerberos development team at MIT said the contents of an unpublished paper with details of this vulnerability have been leaked on the Internet. Using these details, an attacker familiar with Kerberos could easily exploit the vulnerability. Kerberos v4 tickets—or credentials—do not have a cryptographic hash of the encrypted data, random padding or a random initial vector. As a result, using a chosen plaintext attack, an attacker could fabricate a ticket. An attacker who controls a Kerberos cross-realm key would be able to impersonate any principal in the remote realm to any service in that realm. **This attack could lead to a root-level compromise of the Kerberos key distribution center as well as any other hosts that rely on the KDC for authentication.** Kerberos, developed at the Massachusetts Institute of Technology, is among the most widely deployed authentication protocols on the Internet. It is implemented in dozens of software applications, as well, including Windows 2000. However, Windows 2000 uses Kerberos v5 and **Microsoft officials said that, while they're still researching the issue, they don't believe that operating system is vulnerable. Additional information may be found on the MIT Web site:**

<http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2003-004-krb4.txt>

Source: <http://www.eweek.com/article2/0.3959.937375.00.asp>

Internet Alert Dashboard

Current Alert Levels	
 <p>AlertCon: 2 out of 4 https://gtoc.iss.net</p>	 <p>Security Focus ThreatCon: 2 out of 4 http://analyzer.securityfocus.com/</p>
Current Virus and Port Attacks	
Virus:	<p>#1 Virus in the United States: PE_FUNLOVE.4099 Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]</p>
Top 10 Target Ports	<p>80 (www), 137 (netbios-ns), 1434 (ms-sql-m), 113 (ident), 445 (microsoft-ds), 53420 (---), 25 (smtp), 139 (netbios-ssn), 4662 (eDonkey2000), 53 (domain) Source: http://isc.incidents.org/top10.html; Internet Storm Center</p>

[\[Return to top\]](#)

General Sector

36. *March 19, Reuters* — **Mexico increases security amid threat of terrorism.** Mexico said Tuesday that it had deployed about 18,000 troops to increase security on its border with the United States and protect strategic installations against terrorism as war in Iraq looms. **Interior Minister Santiago Creel told reporters that officials in northern border states had formed working groups to help prevent any terrorist infiltration into the United States if, as expected, U.S.-led forces attack Iraq. "They have been alerted and have been in permanent session for several days now," Creel said. Immigration controls at airports, ports and land border crossings have been tightened, he said.** Security at strategic sites such as electricity installations and water plants has also been stepped up, and navy ships are patrolling the coast of Campeche state to protect oil rigs in the Gulf of Mexico owned by state monopoly Pemex.

Source: <http://www.latimes.com/news/nationworld/world/la-war-mexico19mar19.1.697114.story?coll=la%2Dheadlines%2Dworld>

37. *March 19, Washington Post* — **In Detroit, first post-9/11 terrorism trial.** The first trial of terrorism suspects arrested after the Sept. 11, 2001, attacks began in secrecy Tuesday in Detroit, as jury selection began in a case against four defendants that could have a significant impact on the credibility of the Justice Department's war on terrorism, according to legal experts. **The case began Sept. 17, 2001, when federal agents raided the Dearborn apartment searching for Nabil Almarabh, a former Boston cabdriver whose name appeared on an FBI terrorism watch list. They found three other men instead: Farouk Ali-Haimoud, Ahmed Hannan and Karim Koubriti, who said they did not know Almarabh, a former resident.** A search of the apartment netted forged passports, visas, Social Security cards, photos and other fraudulent identity documents, along with 105 audiotapes filled with religious exhortations to kill Christians and Jews. In ensuing months, authorities also apprehended two other suspects: Youssef Hmimssa, a former roommate of the men in the apartment who was wanted on

separate credit card fraud charges, and Abdel-Ilah Elmardoudi, the cell's alleged ringleader. Prosecution documents in the case, which appear to rely heavily on testimony from Hmimssa, portray the four defendants as followers of Salafiya and Takfir wal-Hijra, radical Islamic movements. **The government also alleges that the three Dearborn defendants, who had jobs at Detroit Metropolitan Airport, sought to probe the facility for security gaps.**

Source: http://www.washingtonpost.com/wp-dyn/articles/A49166-2003Mar_18.html

[[Return to top](#)]

DHS/NIPC Products & Contact Information

The Department of Homeland Security's National Infrastructure Protection Center (NIPC) serves as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. The DHS/NIPC provides timely warnings of international threats, comprehensive analysis and law enforcement investigation and response. The NIPC provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the NIPC web-site (<http://www.nipc.gov>), one can quickly access any of the following DHS/NIPC products:

DHS/NIPC Warnings – DHS/NIPC Assessments, Advisories, and Alerts: DHS/NIPC produces three levels of infrastructure warnings which are developed and distributed consistent with the FBI's National Threat Warning System. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/NIPC Publications – DHS/NIPC Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/NIPC Daily Reports Archive – Access past DHS/NIPC Daily Open Source Infrastructure Reports

DHS/NIPC Daily Open Source Infrastructure Report Contact Information

Content and Suggestions: nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/NIPC Daily Report Team at 202-324-1129

Distribution Information: Send mail to nipcdailyadmin@mail.nipc.osis.gov for more information.

Contact DHS/NIPC

To report any incidents or to request information from DHS/NIPC, contact the DHS/NIPC Watch at nipc.watch@fbi.gov or call 202-323-3204.

DHS/NIPC Disclaimer

The DHS/NIPC Daily Open Source Report is a daily [Monday through Friday] summary and assessment of open-source published information concerning significant critical infrastructure issues. This is an internal DHS/NIPC tool intended to serve the informational needs of DHS/NIPC personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The NIPC provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.